Bestanden in een ander bestand verstoppen

Verstoppertje spelen

Iedereen moet wel eens bestanden bewaren of versturen die niet voor jan-en-alleman zichtbaar mogen zijn. Versleutelde bestanden wekken argwaan, maar niemand zal vermoeden dat gewone teksten, foto's of mp3-bestanden de dragers zijn van gevoelig materiaal. Wellicht is dit zelfs een oplossing voor copyright-info. DIRK SCHOOFS



WAT DOEN WE?
- DOCUMENTEN VERSTOPPEN IN TEKSTEN, FOTO'S EN AUDIOBESTANDEN

WAARMEE?
- STEGANOGRAPHY 1.8.1, BON KYU BON EN BDV DATAHIDER

HOELANG?
- ONGEVEER TIEN MINUTEN

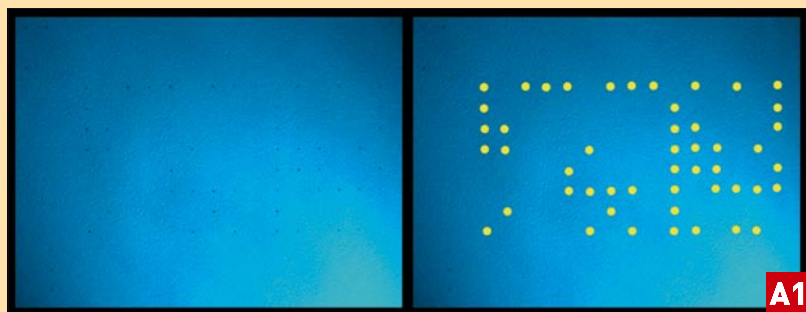
MOEILIJKHEID?



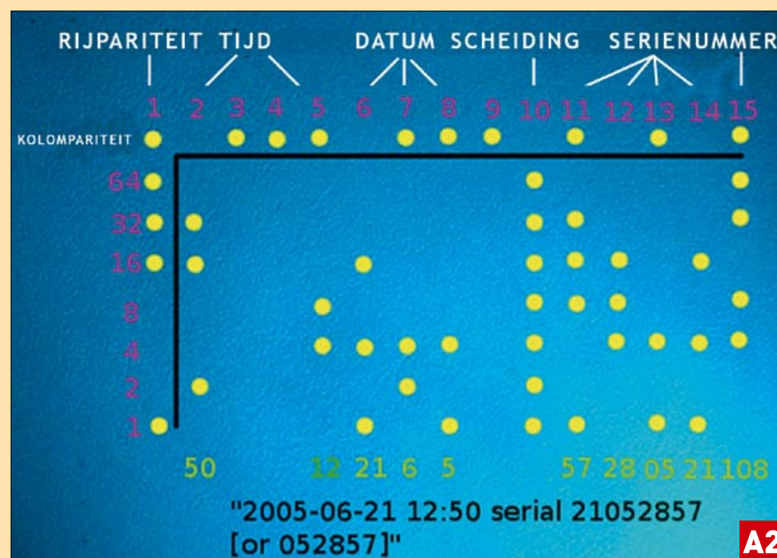
Om te vermijden dat al te nieuwsgierige ogen bepaalde documenten kunnen zien, zijn er twee alternatieven. De eerste optie is boodschappen versleutelen aan de hand van codes. Alleen wie die code kent, kan de boodschap ontcijferen. Een tweede methode is de boodschap op een ongewone plaats neerzetten, zodat niet-ingewijden er klakkeloos aan voorbijgaan. Beide technieken zijn letterlijk zo oud als de straat. De Romeinen werkten al met de Ceasars-code, een geheimtaal (encryptie) waarbij de letters van het alfabet enkele posities werden verplaatst. Het voorbeeld van de tweede methode doet ons denken aan een aflevering van Prison Break, maar dan 440 jaar voor Christus. Toen de Griek Histiaeus gevangen werd gehouden, scheerde hij het hoofd van een slaaf kaal om daar een tatoeage op aan te brengen. De tatoeage waarschuwde de Grieken voor een nakende Perzische invasie. Zodra het haar van de boodschapper gegroeid was, werd de stakker door de vijandelijke linies gestuurd. De methode om informatie op een ongewone manier in het volle zicht te verstoppen, heet steganografie, afkomstig van het Griekse 'steganos' (verborgen) en 'graffein' (schrijven).

A. Verraden door de printer

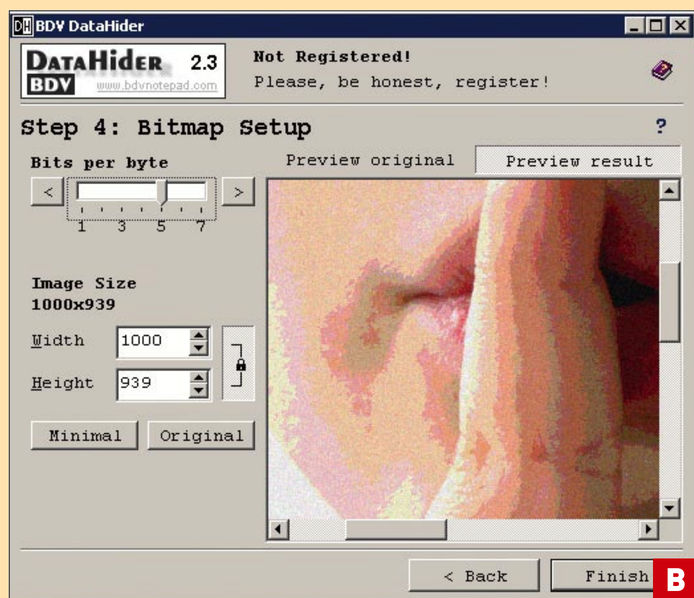
Zowel in de hardware- als in de softwarewereld doen fabrikanten aan encryptie (versleuteling) en steganografie. Moderne laserprinters drukken bijvoorbeeld minuscule gele puntjes op ieder blad papier dat ze verwerken. Met het blote oog kan je deze puntjes nauwelijks zien, maar flink vergroot en onder blauw licht worden ze wel duidelijk (zie afbeelding A1). Het doel is omstreden, en men spreekt zelfs over een inbreuk op de privacy. Het is in ieder geval een soort digitale vingerafdruk van laserprinters. De Amerikaanse inlichtingsdienst maakt van deze code gebruik om valsemunters te klissen. Ondertussen kan iedereen de informatie van die puntjes ontcijferen. De Electronic Frontier Foundation, een Amerikaanse organisatie die zich bekommert om burgerrechten en privacy, heeft dit systeem namelijk gekraakt en legt online uit wat al deze puntjes betekenen www.eff.org/Privacy/printers/wp.php (zie afbeelding A2). Ook de muziekindustrie heeft in zijn strijd tegen de illegale verspreiding van muziek naar het wapen van steganografie gegrepen. Sony plaatste bijvoorbeeld een onhoorbaar signaal dat aangeeft dat het om een originele opname ging.



De mysterieuze puntjes van de laserprinter.



Deze afdruk werd gemaakt op 21 juni '05, op de printer met serienummer 21052857.



In deze ruis verstoppen we andere data.

B. Rekenen op ruis

De basis voor steganografie in digitale bestanden berust op het gegeven dat de menselijke zintuigen beperkt zijn. Wij kunnen kleine onvolmaaktheden niet waarnemen. In alle soorten bestanden die vatbaar zijn voor ruis kan je vreemde bestanden verstoppen (zie afbeelding B). Zo is het mogelijk hele teksten, handleidingen of foto's in mp3-bestanden te verbergen, terwijl die muziek zich nog altijd met iedere mp3-speler laat afspelen. We kunnen bestanden stiekem in digitale foto's stoppen, die we daarna op het web publiceren of over e-mail versturen. Op die manier zou je bijvoorbeeld je copyrightinformatie letterlijk in foto's kunnen plaatsen.

C. Steganography 1.8.1

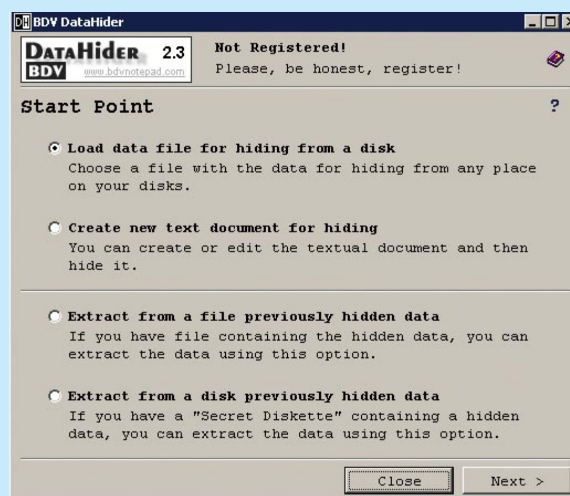
Bespioneert je baas je in- en uitgaand e-mailverkeer? Wil je kattenbelletjes, gedichten of hele liefdesbrieven in een romantische foto verpakken? Of ben je van plan om aan je foto's je naam en adres toe te voegen zonder dat deze gegevens in beeld komen? Wij proberen **Steganography** van www.securekit.com. Het programma kost $ 24,95 (zo'n € 18) en je kan het zeven dagen onbeperkt proberen. Na die zeven dagen kan je met de proefversies nog altijd verstopte informatie tevoorschijn halen, maar het maken van steganografische bestanden is in deze testversie beperkt in de tijd. We nemen de proef op de som met een digitale foto van 1000 bij 939 pixels. Wanneer we de foto als jpg bewaren, hebben we een bestand van 824 KB.

STAP 1 / DEZE WORKSHOP IN EEN FOTO

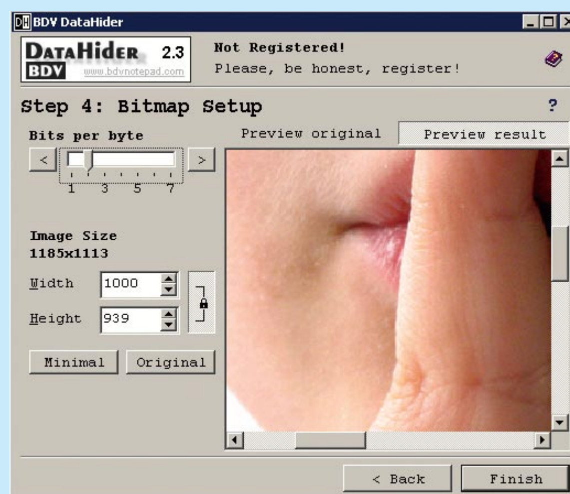
Het programma Steganography werkt in drie stappen. Eerst selecteer je een 'drager', het zogeheten 'carrier file' waar straks andere bestanden in worden verstopt. Vervolgens selecteer je een of meerdere bestanden die in de drager zullen komen. Je hebt de keuze. Ofwel kies je File, ofwel New Message. Opteer je voor het laatste, dan kan je in het volgende tekstvenster de verborgen boodschap intikken of plakken. Kies je voor het eerste, dan navigeer je naar de bedoelde bestanden. We verstoppen de complete tekst van deze workshop via de optie New Message in de foto en merken dat die foto amper 3 KB groter is gewor-

ALTERNATIEVEN

Invisible Secrets4 www.invisiblesecrets.com (zo'n € 28) verbergt jouw diepste geheimen in jpg-, png-, bmp-, html- en wav-formaat. Eigenlijk is dit een totale veiligheidsoplossing om ook e-mail te versleutelen, bestanden definitief van je harde schijf te verwijderen, programma's te beveiligen voor onbevoegden, enzovoort.
Bon Kyu Bon http://web.ist.utl.pt/ist150264/bonkyubon/index.html is Portugese freeware. Deze steganografiesoftware zit nog in een bètastadium en er moet duidelijk nog wat aan de interface gesleuteld worden. Bovendien kan dit programma niet overweg met jpg-bestanden.
De shareware **BDV DataHider 2.3** www.bdvnotepad.com/datahider_en.htm (zo'n € 16) is een uitstekende oplossing. Volg gewoon de wizard in het programma. Het eerste scherm is in twee verdeeld. Het bovenste deel dient om bestanden te vermommen, het onderste deel om verborgen data opnieuw te laten verschijnen. Je kan ofwel een bestaand document verbergen of rechtstreeks in DataHider een tekstbestand aanmaken dat verstopt moet worden. Kies je voor de Bitmap Setup, dan toont het programma hoeveel ruis de 'toegevoegde bits' per byte veroorzaken. Met een schuifregelaar kan je de ruiswaarde instellen van 1 tot 7 bits per byte. In het programma vergelijk je het origineel met het steganografisch bestand en regel je traploos de dosis ruis. Wie overdrijft, krijgt natuurlijk meer ruis dan beeld op zijn bord. Het kan natuurlijk niet de bedoeling zijn dat de vermomming er te dik op ligt.

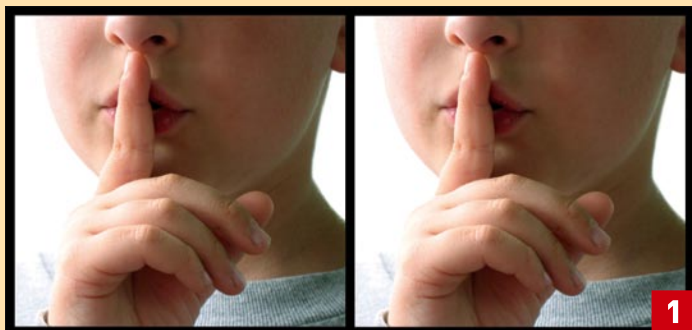


BDV DataHider werkt stapsgewijs met een wizard.



We drijven het aantal nieuwe bits per byte op en houden de beeldkwaliteit voortdurend in het oog.





Links de originele foto, rechts de foto die de complete tekst van deze workshop bevat. Geen verschil!

den. In stap drie kunnen we een wachtwoord ingegeven. Wie de foto later wil openen met dit programma, moet eerst aan de hand van het wachtwoord aantonen dat hij daartoe de bevoegdheid heeft. Wanneer we het origineel én de drager naast elkaar openen, bijvoorbeeld in Photoshop, zien we totaal geen verschil (zie afbeelding 1).

STAP 2 / KRACHTTOEREN

Tijd voor een krachttoer. In plaats van de optie **New Message** zullen we een andere foto in de oorspronkelijke testfoto verstoppen. Het jpg-bestand dat we willen verbergen, is 965 KB groot, dus groter dan de drager. We merken dat het nieuwe uitvoerbestand even groot is als de som van beide bestanden: 966 KB + 825 KB = 1791 KB (zie afbeelding 2a). Nog steeds kunnen we geen extra ruis op het beeldscherm herkennen. De originele foto en drager lijken op ons scherm identiek. We proberen iets spectaculairder. Zouden we dezelfde testfoto ook kunnen verpakken in een mp3-bestand? Jawel, zonder problemen. Alleen aan de bestandsgrootte merken we dat het draagbestand extra data bevat. Maar wie gaat ooit de bestandsgrootte van een mp3 vergelijken met

Naam	Grootte	Type	Gewijzigd op	Afmetingen
Drager.jpg	1.791 kB	Paint Shop Pro X Im...	30/09/2007 14...	1000 x 939
M4J05e.jpg	966 kB	Paint Shop Pro X Im...	26/09/2007 13...	853 x 1280
Testfoto.jpg	825 kB	Paint Shop Pro X Im...	30/09/2007 13...	1000 x 93

2a

De drager is even groot als beide bestanden afzonderlijk.

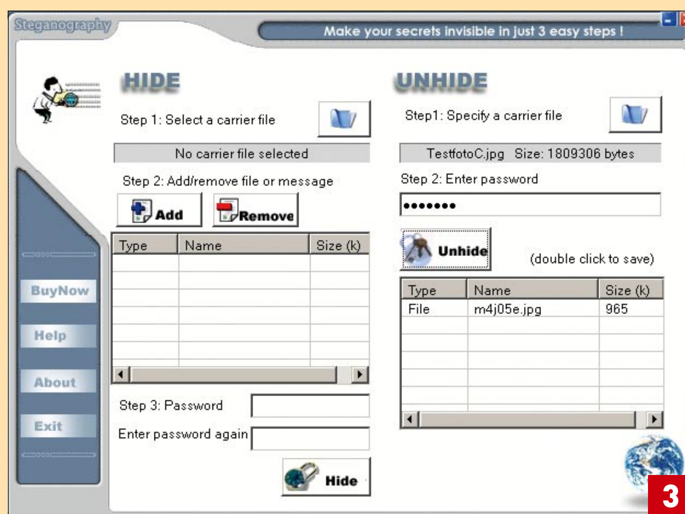


Pure Shores klinkt nog even gaaf, zelfs al zit er een foto van ongeveer 1 MB tussen de muziekdata.

het origineel? Op onze mp3-speler kunnen we evenmin iets van ruis waarnemen (zie afbeelding 2b).

STAP 3 / STEGANALYSE

Het openen van steganografische bestanden noemen we steganalyse. Om de foto's of de informatie opnieuw zichtbaar te maken, open je het programma en gebruik je het rechterdeel van de interface. Eerst het draagbestand selecteren en vervolgens het wachtwoord ingeven en op de **Unhide**-knop klikken (zie afbeelding 3). Ten slotte vraagt het programma naar waar je het bestand wil wegschrijven.



Het verstopte bestand van 965 KB wordt meteen herkend.

D. Watermerken

Wat wint de computergebruiker zonder James Bond-aspiraties bij steganografie? Net zoveel als de industrie die er al jarenlang gebruik van maakt. Heel wat professionele beeldbanken zoals Corbis verkopen hun beelden via het internet en ontvangen geld, afhankelijk van de oplage waarin het beeld verschijnt. Op die manier pikt de fotograaf een graantje mee. Alle foto's worden van een onzichtbaar watermerk voorzien om te vermijden dat het beeld zomaar van eigenaar verwisselt. Op StegoArchive.com http://stegoarchive.com vind je bij **Watermarking Systems** verschillende professionele en amateuroplossingen (zie afbeelding D). Ook met behulp van Steganography of de oplossingen die we in het kaderstuk 'Alternatieven' vermelden, kan je een tekst- of grafisch bestand met copyrightgegevens toevoegen. Zo'n tekstbestand zal de bestandsgrootte nauwelijks wijzigen. ♦



Het StegaArchive, waar je watermerksoftware vindt.